Remarks

The above Amendments and these Remarks are in reply to the Office Action mailed November 1, 2007.

I. Summary of Examiner's Rejections

Claims 1-2, 4-7, 10-12, 18-19, 21-24, 27-29, and 42-43 were pending in the Application prior to the Office Action mailed November 1, 2007. In the Office Action, the Examiner rejected claims 1-2, 4-7, 10-12, 18-19, 21-24, 27-29, and 42-43.

Claims 1, 5, 18, 23, and 42-43 were objected to because of informalities.

Claims 1, 2, 4, 18-19, 21, and 42-43 were rejected under 35 U.S.C. 103(a) as obvious over Sampson (U.S. Patent No. 6,339,423) in view of Sharma (U.S. Patent No. 7, 089,584) further in view of Barkley (US 6,088,679).

Claims 5-7, 10-11, 22-24, and 27-28 were rejected under 35 U.S.C. 103(a) as obvious over Sampson in view of Sharma further in view of Barkley and further in view of Hummel (U.S. Patent No. 6,584,454).

Claims 12 and 29 were rejected under 35 U.S.C. 103(a) as obvious over Sampson in view of Sharma further in view of Barkley further in view of Hummel and further in view of Wiederhold (US 6,226,745).

II. Summary of Applicant's Response

This Reply amends claims 1, 5, 18, 23, and 42-43, and cancels claims 35-39, leaving for the Examiner's present consideration claims 1-2, 4-7, 10-12, 18-19, 21-24, 27-29, and 42-43. The

claims were amended to better define embodiments of Applicant's invention. Reconsideration of the claims is requested.

III. Response to Objections to Claims 1, 5, 18, 23, and 42-43

The amendments to the Claims have rendered the objections moot.

IV. Response to 35 U.S.C. 103(a) Rejections to Claims 1-2, 4-7, 10-12, 18-19, 21-24, and 27-29

Claims 1 and 18

Claim 1 (as amended) states:

A security system for allowing a client to access a protected resource through an application container, the security system comprising:

the application container, which provides services for a protected resource, wherein the application container delegates authorization decisions to a security service by passing an access request and a callback handler to the security service when the application container receives the access request for a protected resource from the client;

context information, wherein the context information comprises one or more parameter values describing the access request, identity of the protected resource, and profile information describing the client;

the security service for making a decision to permit or deny the access request, wherein a plurality of security plug-ins that implement an access decision interface are plugged into the security service, and wherein the plurality of security plug-ins use the callback handler to request the context information from the application container for the access request, and wherein the

plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles is computed dynamically at runtime, and wherein depending on output from each security plug-in the security service determines entitlements for the client to use with the protected resource; and

the security service is located at a first computer, and the protected resource is located either at the first computer or at a second computer.

The Office Action alleges that the combination of Sampson, Sharma, and Barkley suggests the features of Claim 1. Sampson teaches a security system that provides access to resources in multiple domains. Sharma discloses security architecture for integration of Enterprise Information Systems with J2EE. Barkley teaches a workflow system that uses role-based access controls. While Sampson, Sharma, and Barkley are in the field of internet security, applicant respectfully submits that there are significant differences between the features of Claim 1 and the cited documents.

Claim 1 (as amended) requires the plurality of security plug-ins determining roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime. Sampson and Sharma do not suggest having the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime. While Barkley discusses associating roles at run-time, Barkley does not describe many of the features of Claim 1.

Even if the technologies of Barkley, Sampson, and Sharma were combined together, the resulting combination would not look like Claim 1. The resulting hypothetical system as constructed by the Office Action would not have the plurality of security plug-ins using the callback handler to

request context information from the application container. Applicant respectfully submits that the embodiment as defined in Independent Claim 1 is not obvious in view of the combination of Sampson and Sharma. Claim 18 is patentable for similar reasons. Applicant respectfully requests that the 35 U.S.C. § 103(a) rejections to claims 1 and 18 be withdrawn.

Claims 5 and 22

The Office Action alleges that Claim 5's requirement that each of the plurality of security plug-ins can determine a contributory decision to permit, deny, or abstain from the access request is disclosed by Hummel (col 3, lines 4-20). However, the cited portion of Hummel, when combined with Sampson and Sharma, would not result in Applicant's invention as claimed. In Hummel, an agency module intercepts requests for access and contacts a policy server for authenticating passwords. Security codes are authenticated by a security server. Hummel's system divides up tasks amongst different components, Hummel's system does not provide contributory decision-making wherein each security plug-in determines a permit, deny, or abstain for an access request. Furthermore, there is no discussion or suggestion of abstaining from security decisions in Hummel. Hummel does not have a plurality of security plug-ins, instead Hummel only has the policy server.

Claims 6 and 23

The Office Action alleges that Hummel (col . 3, lines 39-60) discloses Claim 6's requirement that the security server further includes an access controller for transferring the access request to the plurality of security plug-ins, and for combining the contributory decisions into an overall decision by the security service to permit or deny the access request. However, the cited portion of Hummel,

when combined with Sampson and Sharma, would not result in Applicant's invention as claimed. In Hummel, some users have a two-factor security clearance, and must enter both a password and a security code for access. In Hummel, the password is authenticated by a policy server and the security code is authenticated by a security server. Hummel has two authentication systems for high-level protected applications, but there is no disclosure or suggestion of combining contributory decisions into an overall decision to permit or deny the access request. Hummel does not have a plurality of security plug-ins, instead it only has the policy server.

Claims 7 and 24

The Office Action alleges that Hummel (col 3, lines 50-60) suggests wherein one or more of the plurality of the security plug-ins represent a business function related access policy. Hummel does not have a plurality of security plug-ins, instead it only has the policy server.

Claims 10 and 27

The Office Action alleges that Hummel (col. 12, lines 25-32) suggests wherein a deny or abstain by any one of the plurality of security plug-ins causes the security service to deny the access request. The cited portion of Hummel does not disclose or suggest a security plug-in that can abstain from making a decision. Furthermore, the cited portion of Hummel does not disclose or suggest a plurality of security plug-ins, instead Hummel teaches a security server that authenticates a security code and then forwards the results of the authentication to a policy server.

Claims 11 and 28

The Office Action alleges that Hummel (col. 3, lines 6-11) suggests wherein an abstain by any one of the plurality of security plug-ins does not cause the security service to deny the access request. The cited portion of Hummel does not suggest a security plug-in that can abstain from making a decision. The Office Action alleges that if the resource/application is open, then the agency module makes a decision to allow access while the policy server is not consulted about the access thereby abstaining from a decision. The Office Action is alleging that if the user is requesting access to an open or unsecured resource, a resource not protected by the policy server, that when the agency module forwards the access request to the web server, that the policy server has somehow abstained from the access decision. In these circumstances, according to Hummel, the policy server is not consulted. Under Hummel, there is no abstaining, the policy server is never asked for a decision.

Claims 42-43

The Office Action asserted that Barkley disclosed Claim 42's requirement that "computation of a dynamic role occurs immediately before an authorization decision for the protected resource." However, Barkley does not appear to disclose this feature. Barkley's col. 9 shows the sequence of steps in Barkley's invention: "Assign permission to perform operation … to ROLEs, Assign ROLESs to USERa, … Sleep, resuming at next line when completion message received…" This statement shows that Barkley's invention was designed to assign roles, sleep while processing commenced, then remove the role assignments after receiving a completion message. Barkley does not, however, appear to disclose computing dynamic role association immediately before an

authorization decision.

Claims 2, 4-7, 10-12, 19, 21-24, 27-29, and 42-43

Dependent Claims 2, 4-7, 10-12, and 42 depend from Claim 1. For at least the reasons discussed above, Dependent Claims 2, 4-7, 10-12, and 42 are patentable. Dependent Claims 2, 4-7, 10-12, and 42 add their own features which render them patentable in their own right. Dependent Claims 19, 21-24, 27-29, and 43 depend from Claim 18. For at least the reasons discussed above, Dependent Claims19, 21-24, 27-29, and 43 are patentable. Dependent Claims 19, 21-24, 27-29, and 43 add their own features which render them patentable in their own right.

V. Conclusion

In light of the above, it is respectfully submitted that all of the claims now pending in the subject patent application should be allowable, and a Notice of Allowance is requested. The Examiner is respectfully requested to telephone the undersigned if he can assist in any way in expediting issuance of a patent.

The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 06-1325 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: February 1, 2008

By: /Thomas K. Plunkett/
Thomas K. Plunkett
Reg. No. 57,253

FLIESLER MEYER LLP
650 California Street, Fourteenth Floor
San Francisco, California 94108
Telephone: (415) 362-3800